RECEIVED
CENTRAL FAX CENTER
JUL 10 2006

STATUS OF THE CLAIMS

The status of the claims is as follows:

1. (Original) A device for supplying output data in reaction to input data, said device comprising:

an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and

a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data,

said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data.

2. (Original) A device according to claim 1, wherein the operational data are selected from the group comprising time data and power data.

3. (Original) A device according to claim 1, wherein the electronic circuit and the detection unit are integrated as a unit.

4. (Original) A device according to claim 1, which is contained in a smart card or in a PC card.

5. (Original) A device according to claim 1, wherein the electronic circuit is arranged so as to execute an cryptoalgorithm.

6. (Original) A device according to claim 1, wherein the electronic circuit is arranged so as to execute a check sum algorithm.

7. (Original) A device according to claim 5, wherein the cryptoalgorithm is a multi-step algorithm, the operational data of one algorithm step being used as input data for the subsequent algorithm step.

8. (Original) A device according to claim 1, wherein the electronic circuit is arranged so as to stop the operation after a predetermined execution time during execution of the algorithm and wherein the detection unit is arranged so as to feed operational data into the algorithm at said predetermined execution time.

9. (Original) A device according to claim 1, wherein the algorithm is of such a nature that it will first randomize the input data, whereby the dependence of the operational data on the input data will be pseudo-random.

10. (Original) A device according to claim 9, wherein the output data generated by the algorithm are only the operational data.

11. (Original) A device according to claim 1, wherein the electronic circuit comprises two sub-circuits which each execute a sub-algorithm, the first sub-algorithm being a test algorithm whose operational data are detected by the detection unit, and the second sub-algorithm being a cryptoalgorithm or a check sum algorithm, the operational data of the test algorithm being processed in the cryptoalgorithm.

12. (Original) A device according to claim 11, wherein the second sub-circuit is arranged so as to execute the DES algorithm which comprises n steps, and wherein the first sub-circuit is arranged so as to execute a test algorithm which also comprises n steps, the input data being adapted to be fed into the first step of the DES algorithm as well as into the first step of the test algorithm, and data which are adapted to be fed into a further step of the DES algorithm being result data of the first step of the DES algorithm and operational data of the first step of the test algorithm, whereas a result of one step of the test algorithm is rejected.

COPY

13. (Original) A device according to claim 1, wherein the operational data detection unit comprises a time measuring means and a power measuring means for measuring the time which the electronic circuit needs for executing a specific task and for measuring the power consumed when said specific task is being executed.

14. (Original) A device according to claim 13, wherein the power measuring means comprises a resistor, a capacitor and an analog-digital converter for measuring the power consumed.

15. (Original) A device according to claim 13, wherein the time measuring means comprises an internal clock generator.

16. (Original) A device according to claim 1, wherein the operational data detection unit comprises a pattern recognition algorithm so as to produce the operational data from power or time parameters of the electronic circuit.

17. (Original) A method for checking the authenticity of a device to be tested in comparison with an examination device, the device to be tested and the examination device each comprising an electronic circuit for executing an algorithm, which generates output data on the basis of input data, and a unit for detecting operational data which are influenced by an operation of the electronic circuit and which depend on the input data, the operational data detection unit of the device to be tested as well as of the examination device being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm for producing the output data, said method comprising the following steps:

selecting input data;

feeding said input data into the device to be tested;

in the device to be tested,

executing the algorithm by the electronic circuit of the device to be tested, so as to generate the output data on the basis of the input data,

COPY

detecting operational data of the electronic circuit, which are influenced by an operation of said electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data;

feeding the input data into the examination device;

in the examination device

executing the algorithm by the electronic circuit of the examination device so as to generate the output data on the basis of the input data,

detecting operational data of the electronic circuit, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data;

comparing the output data of the device to be tested with the output data of the examination device; and

affirming the authenticity of the device to be tested in comparison with the examination device if the output data correspond to one another, in such a way that authenticity will only be affirmed if the operational data of the device to be tested and of the examination device correspond to one another.

18. (Original) A method for encrypted transmission of information from a first to a second location, the second location being remote from the first location, comprising:

producing a random word;

feeding the random word into a first device the first device comprising an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said

electronic circuit, for generating the output data, the first device being arranged at a first location;

generating the output data of the first device, which depend on the operational data of said first device, by executing an algorithm by the electronic circuit of said first device so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data;

encrypting the information with the generated output data as a key;

transmitting the encrypted information and the random word from said first location to said second location;

feeding the random word into a second device, the second device comprising an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data, the second device being positioned at the second location;

generating the output data of the second device, which depend on the operational data of said second device, by executing the algorithm by the electronic circuit of said second device, so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data;

decrypting the encrypted information making use of the output data of the second device as a key,

the decrypted information corresponding to the original information prior to encrypting if the operational data of the first device at the first location correspond to the operational data of the second device at the second location.